무선 LAN 컨트롤러 및 ID 서비스 엔진을 통한 EAP-FAST 인증

목차

소개

이 문서에서는 외부 RADIUS 서버를 사용하여 EAP(Extensible Authentication Protocol) - FAST(Flexible Authentication via Secure Tunneling) 인증을 위한 WLC(Wireless LAN Controller)를 구성하는 방법에 대해 설명합니다.이 컨피그레이션 예에서는 ISE(Identity Services Engine)를 외부 RADIUS 서버로 사용하여 무선 클라이언트를 인증합니다.

이 문서에서는 무선 클라이언트에 대한 익명 및 인증된 대역 내(자동) 보호 액세스 자격 증명(PAC) 프로비저닝을 위한 ISE를 구성하는 방법에 초점을 맞춥니다.

사전 요구 사항

요구 사항

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- LAP(Lightweight Access Point) 및 Cisco WLC의 구성에 대한 기본 지식
- CAPWAP 프로토콜에 대한 기본 지식
- Cisco ISE와 같은 외부 RADIUS 서버를 구성하는 방법에 대한 지식
- 일반 EAP 프레임워크에 대한 기능 지식
- MS-CHAPv2 및 EAP-GTC 같은 보안 프로토콜에 대한 기본 지식 및 디지털 인증서에 대한 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 펌웨어 릴리스 8.8.111.0을 실행하는 Cisco 5520 Series WLCCisco 4800 Series APAnyConnect NAM입니다.Cisco Secure ISE 버전 2.3.0.298버전 15.2(4)E1을 실행하는 Cisco 3560-CX Series 스위치

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

배경 정보

EAP-FAST 프로토콜은 Cisco가 강력한 비밀번호 정책을 적용할 수 없고 디지털 인증서가 필요하지 않은 802.1X EAP 유형을 구축하려는 고객을 지원하기 위해 개발한 공개적으로 액세스 가능한 IEEE 802.1X EAP 유형입니다.

EAP-FAST 프로토콜은 TLS(Transport Level Security) 터널을 사용하여 EAP 트랜잭션을 암호화하는 클라이언트 서버 보안 아키텍처입니다.EAP-FAST 터널 설정은 사용자에게 고유한 강력한 암호를 기반으로 합니다.이러한 강력한 기밀은 ISE에만 알려진 마스터 키를 사용하여 ISE가 생성하는 PACs라고 합니다.

EAP-FAST는 다음 3단계로 이루어집니다.

- **단계 0(자동 PAC 프로비저닝 단계)**—EAP-FAST 단계 0, 선택적 단계는 네트워크 액세스를 요청하는 사용자를 위한 PAC를 EAP-FAST 최종 사용자 클라이언트에 제공하는 터널 보안 방법입니다.**최종 사용자 클라이언트에 PAC를 제공하는 것은 제로 단계의 유일한 목적입니다.참고:** PAC는 0단계를 사용하는 대신 클라이언트에 수동으로 프로비저닝할 수 있으므로 0단계는 선택 사항입니다.자세한 내용은 이 문서의 PAC 프로비저닝 모드 섹션을 참조하십시오.
- **1단계** - 1단계에서 ISE와 최종 사용자 클라이언트는 사용자의 PAC 자격 증명을 기반으로 TLS 터널을 설정합니다.이 단계에서는 최종 사용자 클라이언트가 네트워크 액세스를 시도하는 사용자에 대해 PAC를 제공하고 PAC가 만료되지 않은 마스터 키를 기반으로 해야 합니다.EAP-FAST 중 1단계에서 네트워크 서비스를 활성화하지 않습니다.
- **2단계** - 2단계에서 사용자 인증 자격 증명은 TLS 터널 내에서 EAP-FAST에서 지원하는 내부 EAP 방법을 사용하여 클라이언트와 RADIUS 서버 간의 PAC를 사용하여 생성된 RADIUS로 안

전하게 전달됩니다.EAP-GTC, TLS 및 MS-CHAP는 내부 EAP 방법으로 지원됩니다.EAP-FAST에 대해 다른 EAP 유형은 지원되지 않습니다.

자세한 내용은 EAP-FAST 작동 방식을 참조하십시오.

PAC

PAC는 ISE와 EAP-FAST 최종 사용자 클라이언트가 서로 인증하고 EAP-FAST 2단계에서 사용할 TLS 터널을 설정할 수 있도록 하는 강력한 공유 비밀입니다.ISE는 활성 마스터 키와 사용자 이름을 사용하여 PAC를 생성합니다.

PAC는 다음과 같이 구성됩니다.

- **PAC-Key** - 클라이언트(및 클라이언트 디바이스) 및 서버 ID에 바인딩된 공유 암호입니다.
- **PAC Opaque**(PAC 불투명) - 클라이언트가 캐시하고 서버에 전달하는 불투명 필드입니다.서버는 PAC-Key 및 클라이언트 ID를 복구하여 클라이언트와 상호 인증합니다.
- **PAC-Info** - 클라이언트가 다른 PAC를 캐시할 수 있도록 최소한 서버의 ID를 포함합니다.선택적으로, PAC의 만료 시간과 같은 다른 정보를 포함합니다.

PAC 프로비저닝 모드

앞에서 언급했듯이, 단계 0은 선택적인 단계입니다.

EAP-FAST는 PAC로 클라이언트를 프로비저닝하기 위한 두 가지 옵션을 제공합니다.

- **자동 PAC 프로비저닝(EAP-FAST 단계 0 또는 대역 내 PAC 프로비저닝)**
- **수동(대역 외) PAC 프로비저닝**

대역 내/자동 PAC 프로비저닝은 보안 네트워크 연결을 통해 최종 사용자 클라이언트에 새 PAC를 전송합니다.자동 PAC 프로비저닝은 자동 프로비저닝을 지원하도록 ISE 및 최종 사용자 클라이언트를 구성하는 경우 네트워크 사용자 또는 ISE 관리자의 개입 없이 이루어집니다.

최신 EAP-FAST 버전은 두 가지 다른 인밴드 PAC 프로비저닝 구성 옵션을 지원합니다.

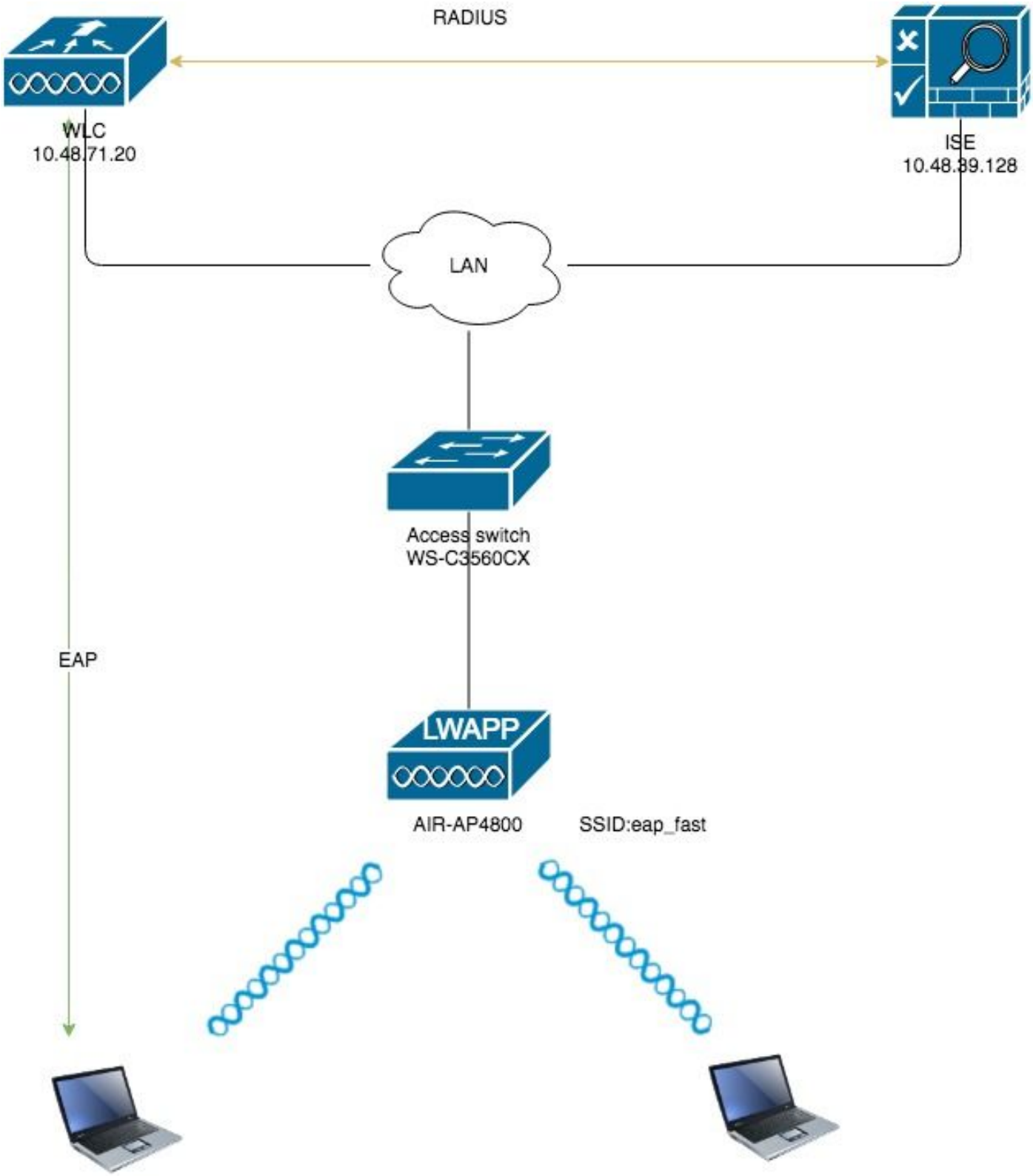
- **익명 대역 내 PAC 프로비저닝**
- **인증된 대역 내 PAC 프로비저닝**

참고: 이 문서에서는 이러한 인밴드 PAC 프로비저닝 방법과 이를 구성하는 방법에 대해 설명합니다.

대역 외/수동 PAC 프로비저닝을 수행하려면 ISE 관리자가 PAC 파일을 생성해야 합니다. 그러면 해당 네트워크 사용자에게 배포되어야 합니다.사용자는 PAC 파일로 최종 사용자 클라이언트를 구성해야 합니다.

구성

네트워크 다이어그램



구성

EAP-FAST 인증을 위한 WLC 구성

EAP-FAST 인증을 위한 WLC를 구성하려면 다음 단계를 수행합니다.

1. 외부 RADIUS 서버를 통해 RADIUS 인증을 위한 WLC 구성
2. EAP-FAST 인증을 위한 WLAN 구성

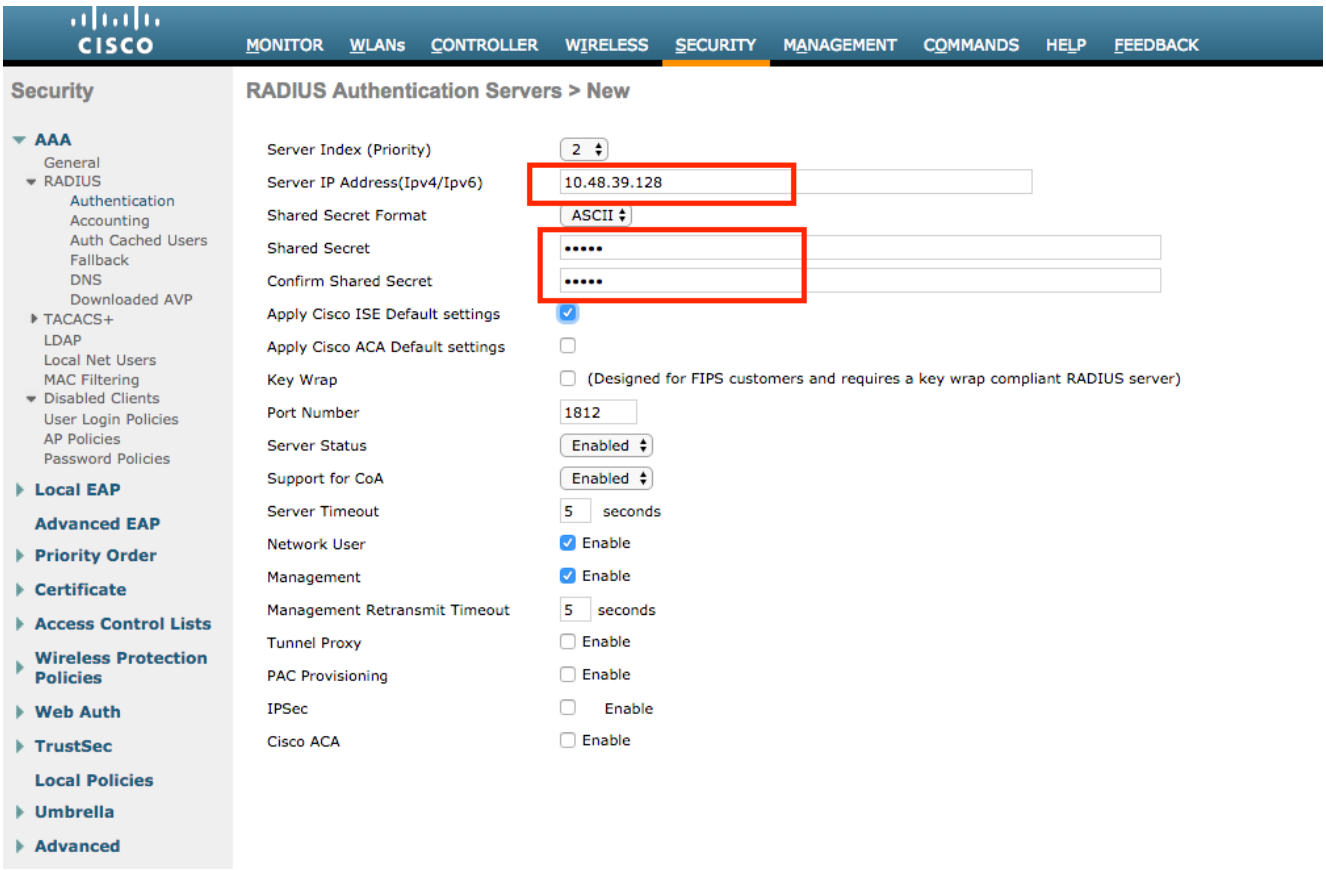
외부 RADIUS 서버를 통해 RADIUS 인증을 위한 WLC 구성

사용자 자격 증명을 외부 RADIUS 서버로 전달하려면 WLC를 구성해야 합니다.그런 다음 외부 RADIUS 서버는 EAP-FAST를 사용하여 사용자 자격 증명을 확인하고 무선 클라이언트에 대한 액세스를 제공합니다.

외부 RADIUS 서버에 대해 WLC를 구성하려면 다음 단계를 완료합니다.

1. RADIUS **Authentication** Servers(RADIUS **인증 서버**) 페이지를 표시하려면 컨트롤러 GUI에서 Security(보안) 및 RADIUS Authentication(RADIUS 인증 서버)을 선택합니다.그런 다음 **New(새로 만들기)**를 클릭하여 RADIUS 서버를 정의합니다.
2. RADIUS Authentication Servers(RADIUS 인증 서버) **> New(새** 페이지)**에서 RADIUS** 서버 매개변수**를** 정의합니다.이러한 매개변수는 다음과 같습니다.RADIUS 서버 IP 주소공유 암호포트 번호서버 상태이 문서에서는 IP 주소가 10.48.39.128인 ISE 서버를 사용합니다

.



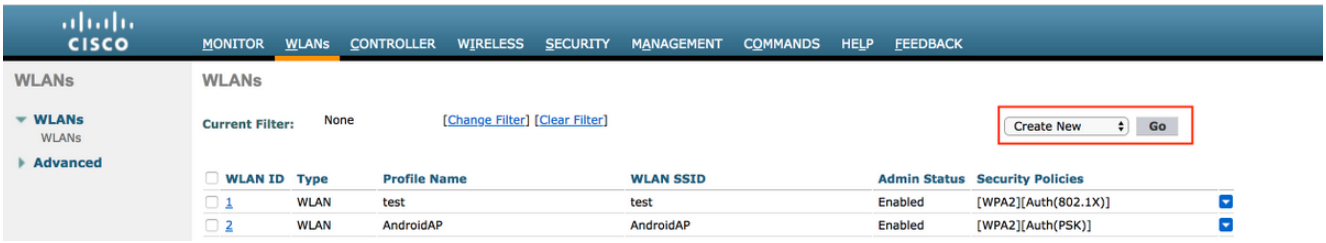
3. 클릭 **적용**.

EAP-FAST 인증을 위한 WLAN 구성

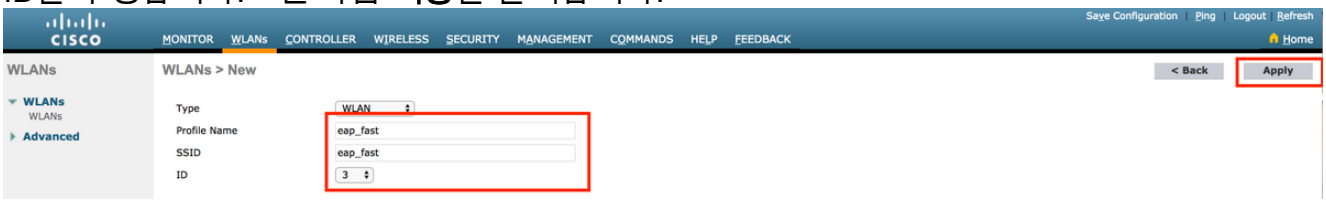
다음으로, 클라이언트가 EAP-FAST 인증을 위해 무선 네트워크에 연결하고 동적 인터페이스에 할당하는 데 사용하는 WLAN을 구성합니다.이 예에서 구성된 WLAN 이름은 eap **fast**입니다.이 예에서는 관리 인터페이스에 이 WLAN을 할당합니다.

eap **fast** WLAN 및 관련 매개변수를 구성하려면 다음 단계를 완료합니다.

1. WLANs 페이지를 표시하려면 컨트롤러의 GUI에서 WLANs를 클릭합니다.이 페이지에는 컨트롤러에 있는 WLAN이 나열됩니다.
2. 새 WLAN을 생성하려면 **New**(새로 만들기)를 클릭합니다.

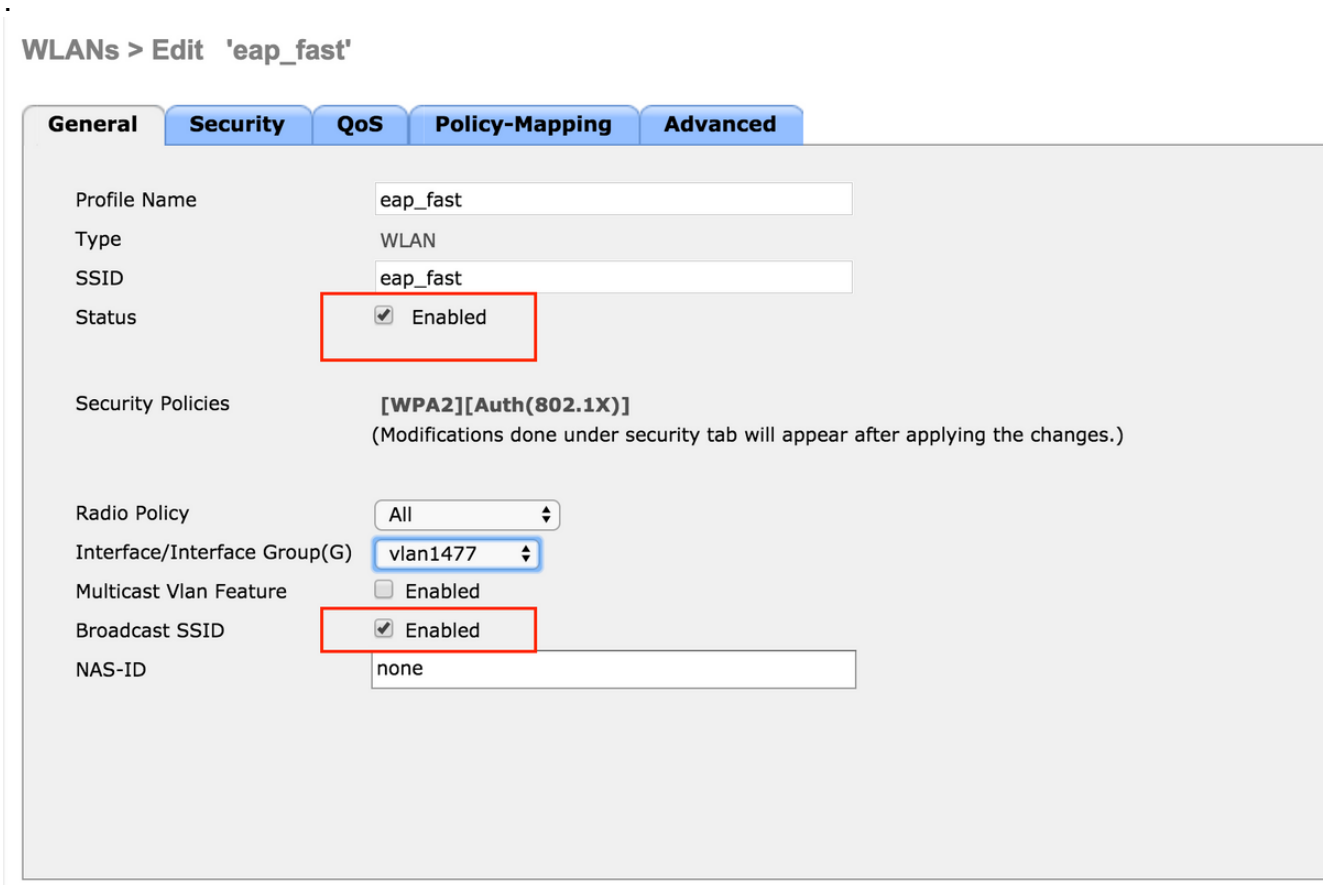


3. WLANs(WLAN) > New(새 페이지)에서 eap_fast WLAN SSID 이름, 프로파일 이름 및 WLAN ID를 구성합니다.그런 다음 **적용**을 클릭합니다.

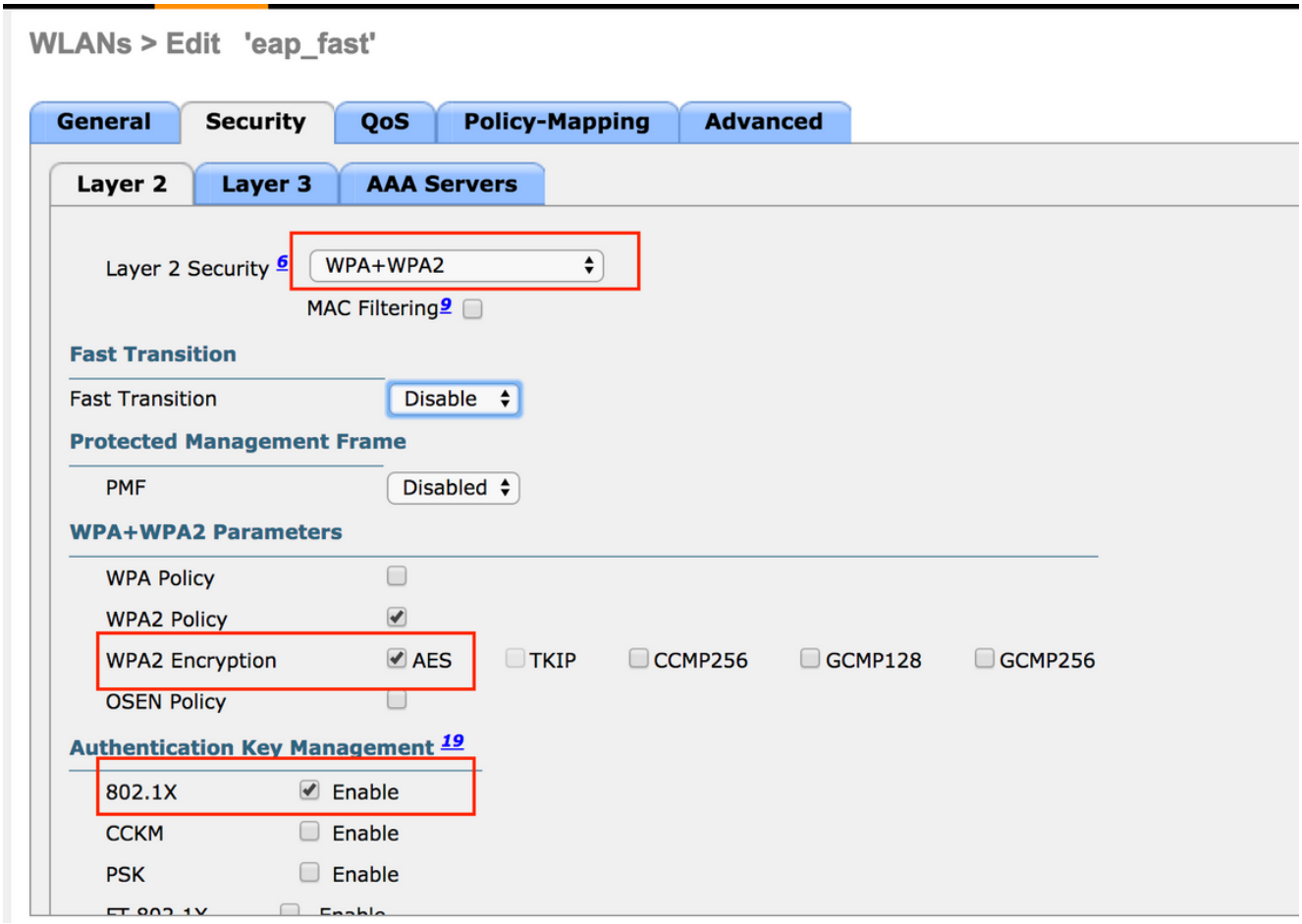


4. 새 WLAN을 생성하면 새 WLAN에 대한 **WLAN > Edit** 페이지가 나타납니다.이 페이지에서 이 WLAN에 특정한 다양한 매개변수를 정의할 수 있습니다.여기에는 일반 정책, RADIUS 서버, 보안 정책 및 802.1x 매개변수가 포함됩니다.
5. WLAN을 활성화하려면 **General** Policies(**일반 정책**) 탭 아래의 Admin Status(관리 상태) 확인란을 선택합니다.AP가 해당 비컨 프레임에서 SSID를 브로드캐스트하도록 하려면 Broadcast **SSID** 확인란을 선택합니다

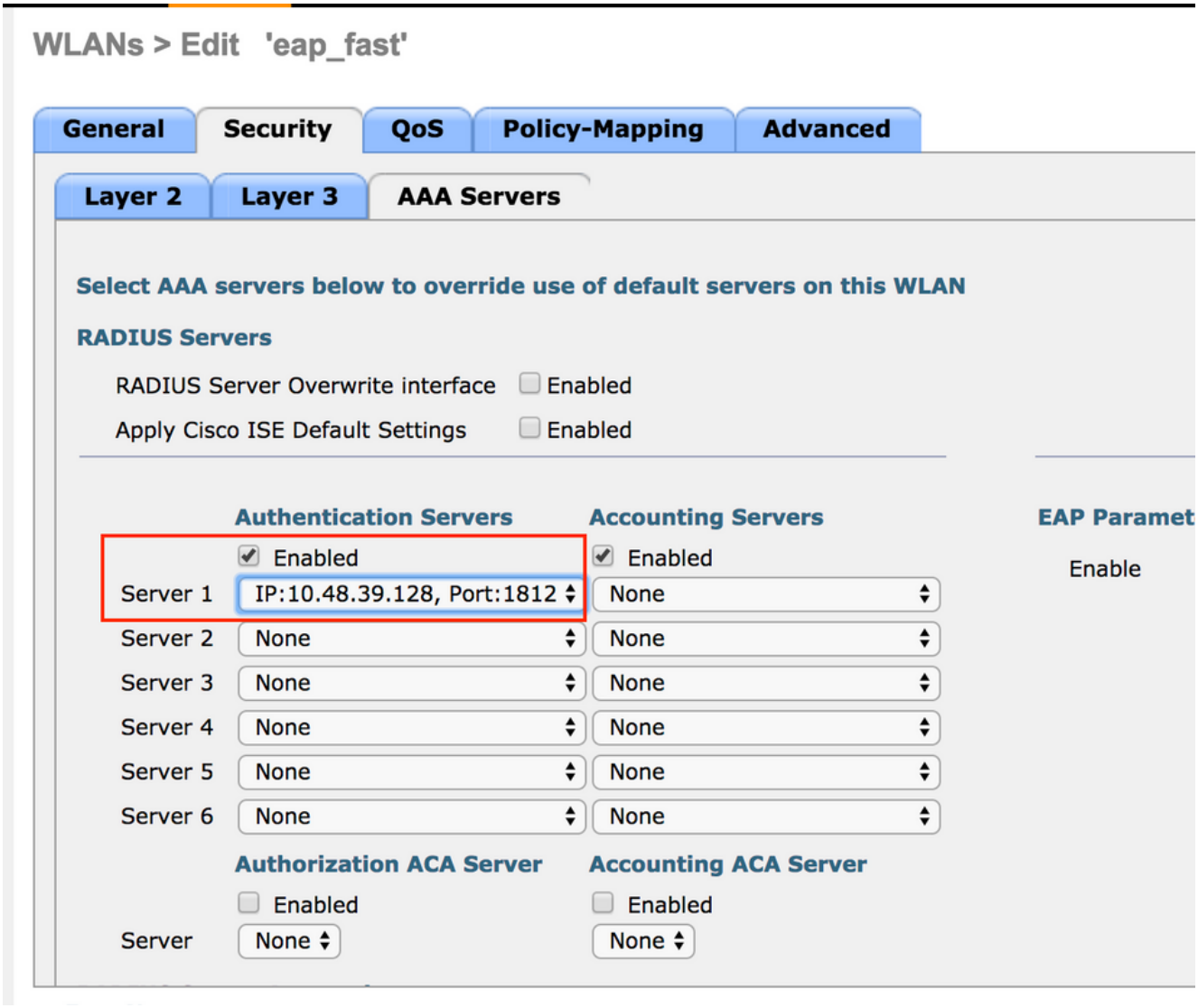
.



6. 아래 **"WLAN -> Edit -> Security -> Layer 2"** 탭 WPA/WPA2 매개변수를 선택하고 AKM에 대해 dot1x를 선택합니다.
   이 예에서는 이 WLAN에 대한 레이어 2 보안으로 WPA2/AES + dot1x를 사용합니다.다른 매개변수는 WLAN 네트워크의 요구 사항에 따라 수정할 수 있습니다.



7. **"WLAN -> Edit -> Security -> AAA Servers(WLAN -> 보안 -> AAA 서버)"** 탭에서 RADIUS Servers(RADIUS 서버) 아래의 풀다운 메뉴에서 적절한 RADIUS 서버를 선택합니다.



8. Apply를 **클릭합니다.참고:** EAP 인증을 위해 컨트롤러에서 구성해야 하는 유일한 EAP 설정입니다.EAP-FAST와 관련된 다른 모든 컨피그레이션은 RADIUS 서버 및 인증해야 하는 클라이언트에서 수행해야 합니다.

EAP-FAST 인증을 위한 RADIUS 서버 구성

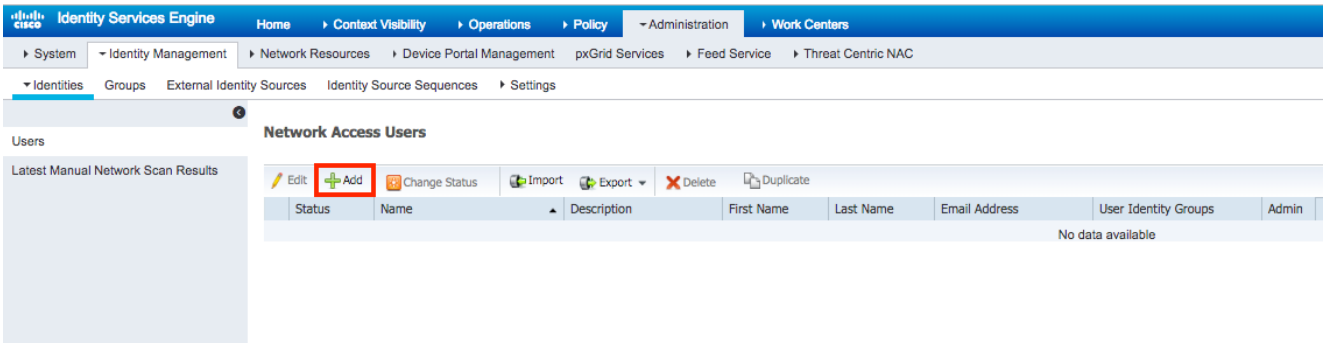
EAP-FAST 인증을 위해 RADIUS 서버를 구성하려면 다음 단계를 수행합니다.

1. EAP-FAST 클라이언트를 인증하는 사용자 데이터베이스 생성
2. RADIUS 서버에 AAA 클라이언트로 WLC 추가
3. 익명 대역 내 PAC 프로비저닝을 사용하여 RADIUS 서버에 EAP-FAST 인증 구성
4. 인증된 대역 내 PAC 프로비저닝을 사용하여 RADIUS 서버에 EAP-FAST 인증 구성

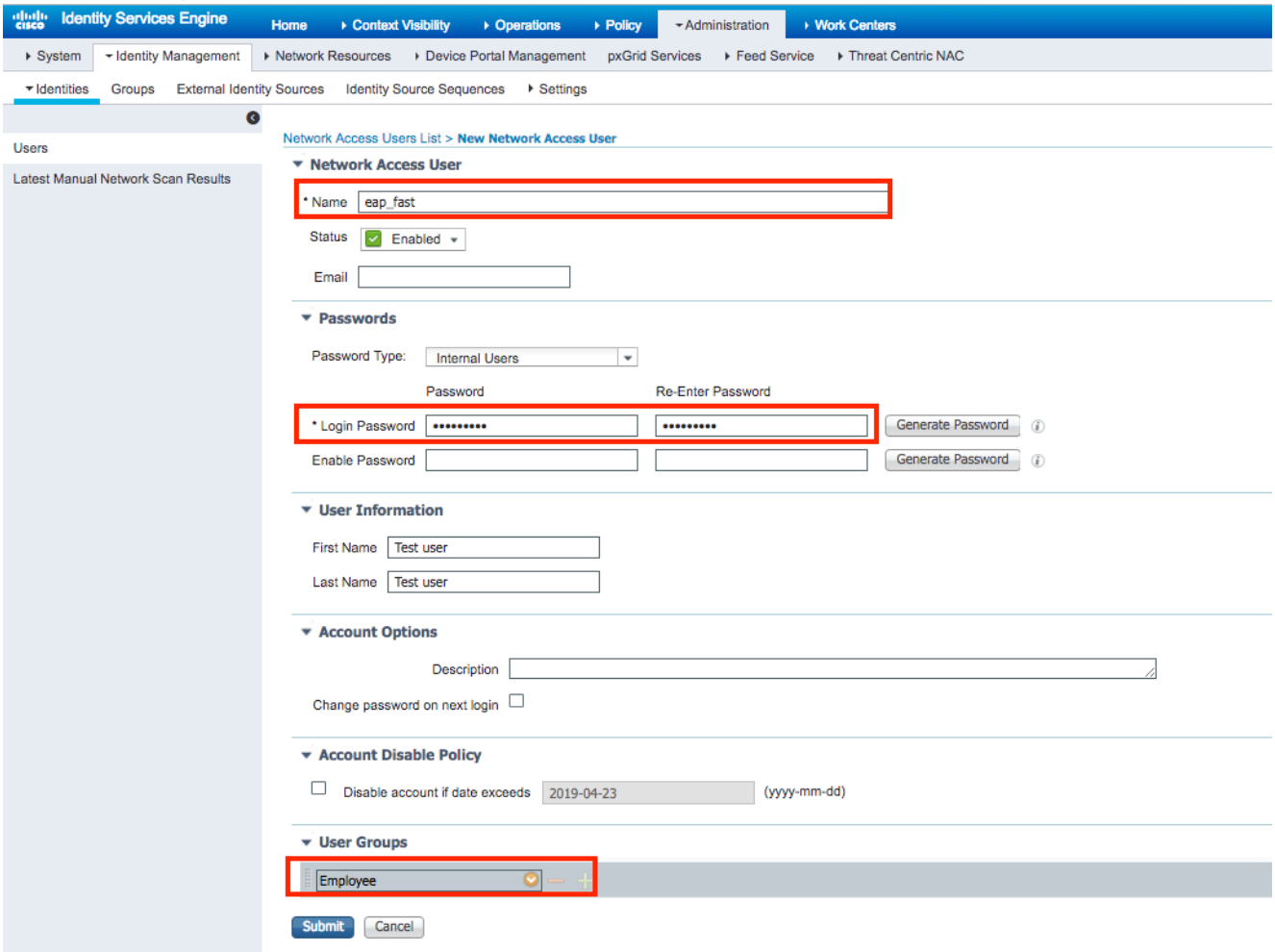
EAP-FAST 클라이언트를 인증하는 사용자 데이터베이스 생성

이 예에서는 EAP-FAST 클라이언트의 사용자 이름 및 비밀번호를 각각 <*eap_fast*> 및 <*EAP-fast1*>으로 구성합니다.

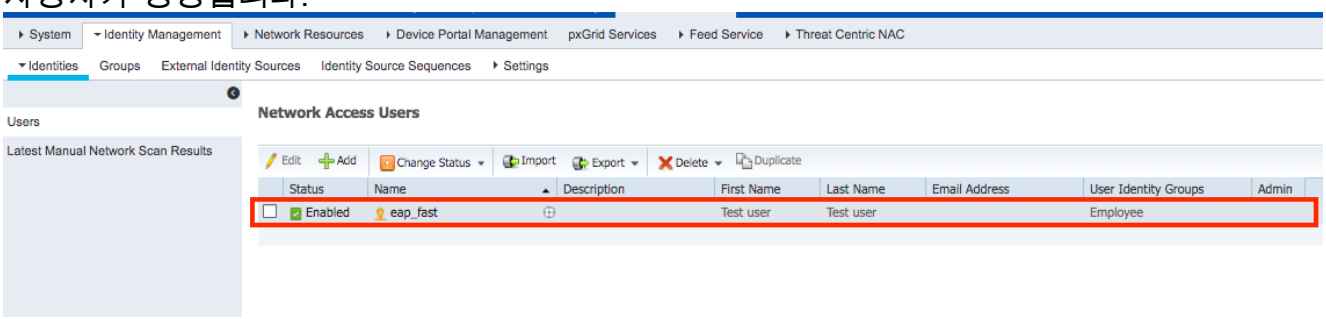
1. ISE 웹 관리 UI에서 **"Administration -> Identity Management -> Users"(관리 -> ID 관리 -> 사용자)"** 아래에서 **"Add(추가)"** 아이콘을 누릅니다.



2. "**Name**" 및 "**Login password**" 사용자를 만드는 데 필요한 양식을 입력하고 드롭다운 목록에서 "User group"을 선택합니다.[선택적으로 사용자 계정에 대한 다른 정보를 입력할 수 있습니다.]
"Sumbit(요약)"를 누릅니다.



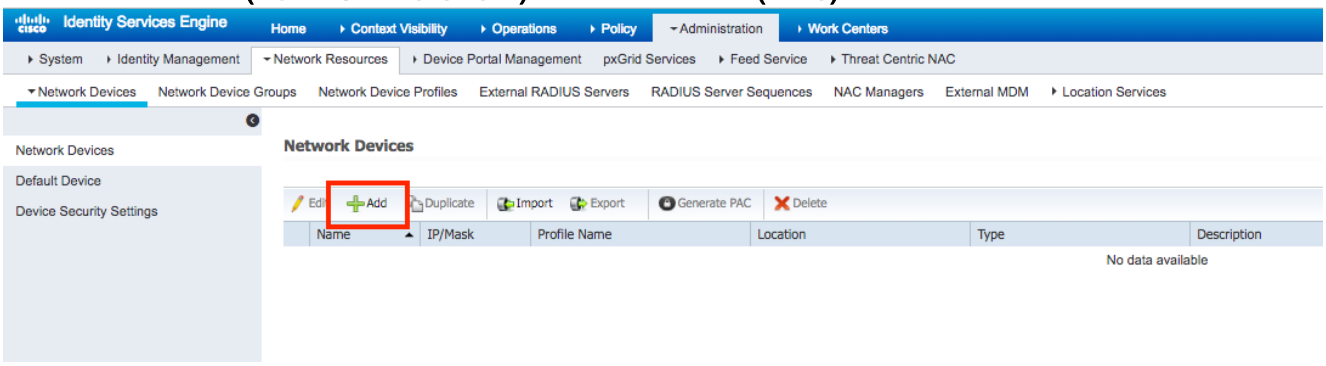
3. 사용자가 생성됩니다.



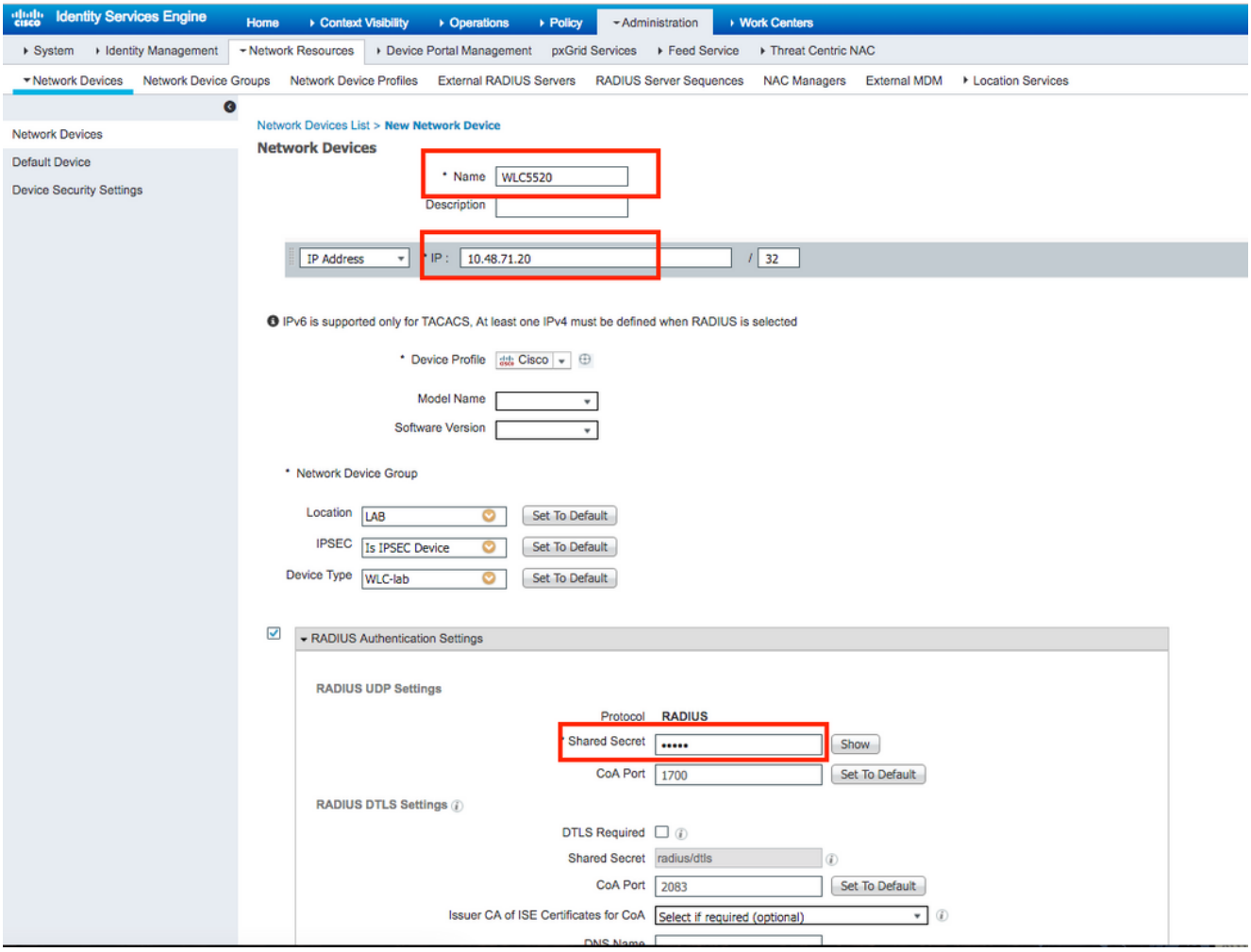
RADIUS 서버에 AAA 클라이언트로 WLC 추가

컨트롤러를 ACS 서버에서 AAA 클라이언트로 정의하려면 다음 단계를 완료하십시오.

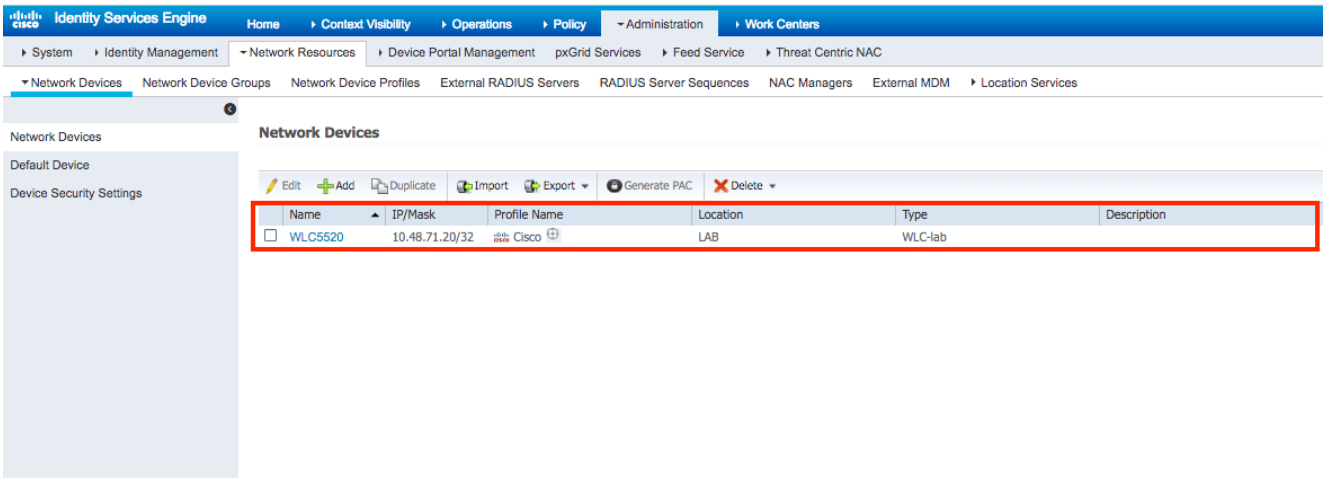
1. ISE 웹 관리 UI에서 **"Administration(관리) -> Network Resources(네트워크 리소스) -> Network Devices(네트워크 디바이스)"** 아래에서 **"Add(추가)"** 아이콘을 누릅니다.



2. 추가할 디바이스에 필요한 양식(**"Name"**, **"IP"**)을 입력하고 이전 섹션에서 WLC에 구성한 것과 동일한 공유 암호 암호를 **"Shared Secret"** 양식 [선택 사항에 위치, 그룹 등 디바이스에 대한 다른 정보를 입력할 수 있습니다.]
"Sumbit(요약)"**를 누릅니다**.



3. 디바이스가 ISE 네트워크 액세스 디바이스 목록에 추가됩니다.(NAD)

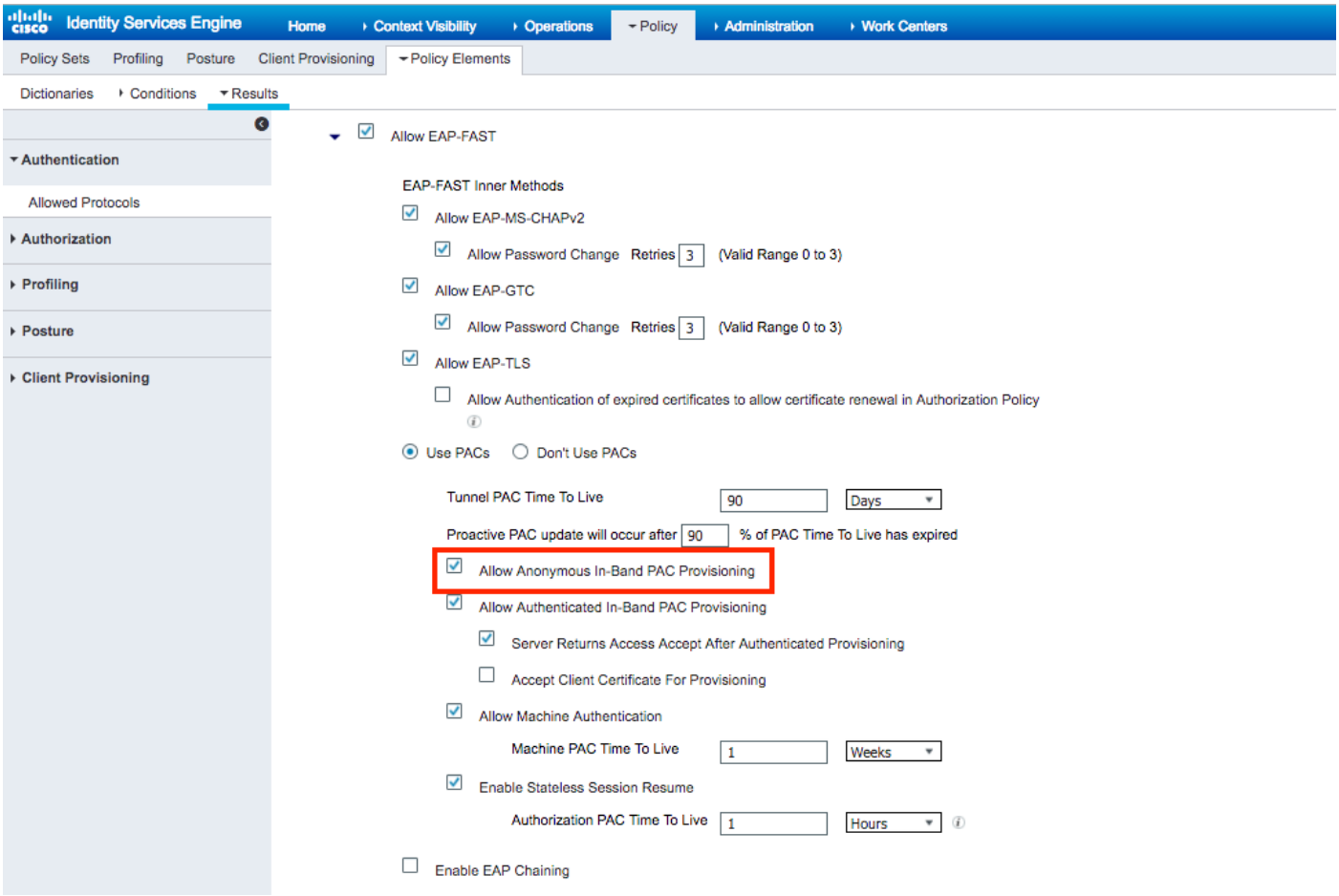


익명 대역 내 PAC 프로비저닝을 사용하여 RADIUS 서버에 EAP-FAST 인증 구성

일반적으로 구축 시 PKI 인프라가 없을 경우 이 유형의 방법을 사용하고자 합니다.

이 방법은 피어가 ISE 서버를 인증하기 전에 ADHP(Authenticated Diffie-HellmanKey Agreement Protocol) 터널 내에서 작동합니다.

이 방법을 지원하려면 "Authentication Allowed Protocols(**인증 허용 프로토콜**)"에서 ISE에서 ""**Allow Anonymous In-band PAC Provisioning(익명 대역 내 PAC 프로비저닝 허용)**"을 활성화해야 합니다.



참고: EAP-FAST 내부 방법에 대해 EAP-MS-CHAPv2 같은 비밀번호 유형 인증을 허용했는지 확인하십시오. 익명 대역 내 프로비저닝에서는 인증서를 사용할 수 없기 때문입니다.

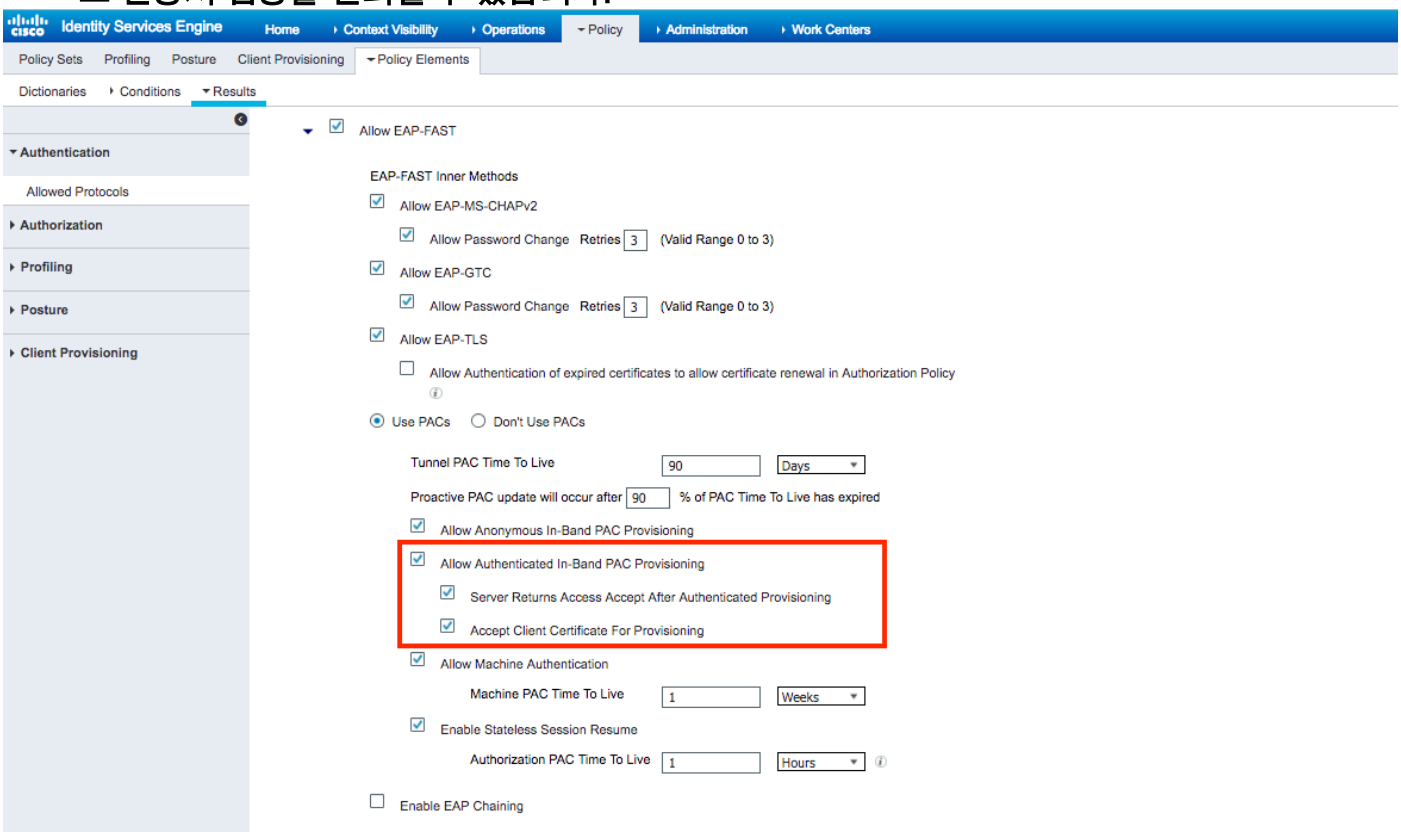
인증된 대역 내 PAC 프로비저닝을 사용하여 RADIUS 서버에 EAP-FAST 인증 구성

가장 안전하고 권장되는 옵션입니다.TLS 터널은 서 플리 컨 트에 의해 확인 된 서버 인증서를 기반으로 구축되며 클라이언트 인증서는 ISE (기본값)에 의해 확인 됩니다.

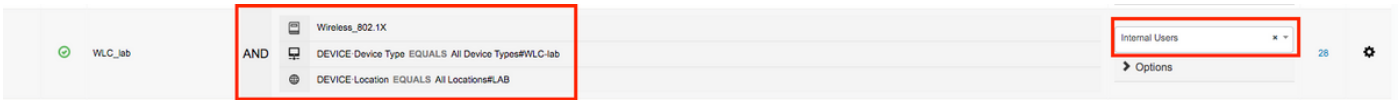
이 옵션을 사용하려면 클라이언트 및 서버용 PKI 인프라가 있어야 합니다. 단, 서버 측으로만 제한되거나 양쪽에서 건너뛸 수 있습니다.

ISE에는 인증된 대역 내 프로비저닝에 대한 두 가지 추가 옵션이 있습니다.

1. **"Server Returns Access Accept After Authenticated Provisioning(서버가 인증된 프로비저닝 후 액세스 수락 반환)"** - 일반적으로 PAC 프로비저닝 후 액세스 거부를 전송하여 신청자가 PAC를 사용하여 재인증하도록 해야 합니다.그러나 PAC 프로비저닝은 인증된 TLS 터널에서 수행되므로 Access-Accept로 신속하게 응답하여 인증 시간을 최소화할 수 있습니다.(이 경우 클라이언트 및 서버 쪽에 신뢰할 수 있는 인증서가 있는지 확인하십시오.)
2. **"프로비저닝을 위한 클라이언트 인증서 수락" - 클라이언트 디바이스에 PKI 인프라를 제공하지 않고 ISE에 신뢰할 수 있는 인증서만 있으면 해당 옵션을 활성화하여 서버 측에서 클라이언트 인증서 검증을 건너뛸 수 있습니다.**



또한 ISE에서는 무선 사용자에 대한 단순 인증 정책 집합을 정의합니다. 아래의 예는 조건 매개 변수 장치 유형 및 위치 및 인증 유형으로 를 사용하고 있습니다. 이 조건과 일치하는 인증 흐름은 내부 사용자 데이터베이스에 대해 검증됩니다.



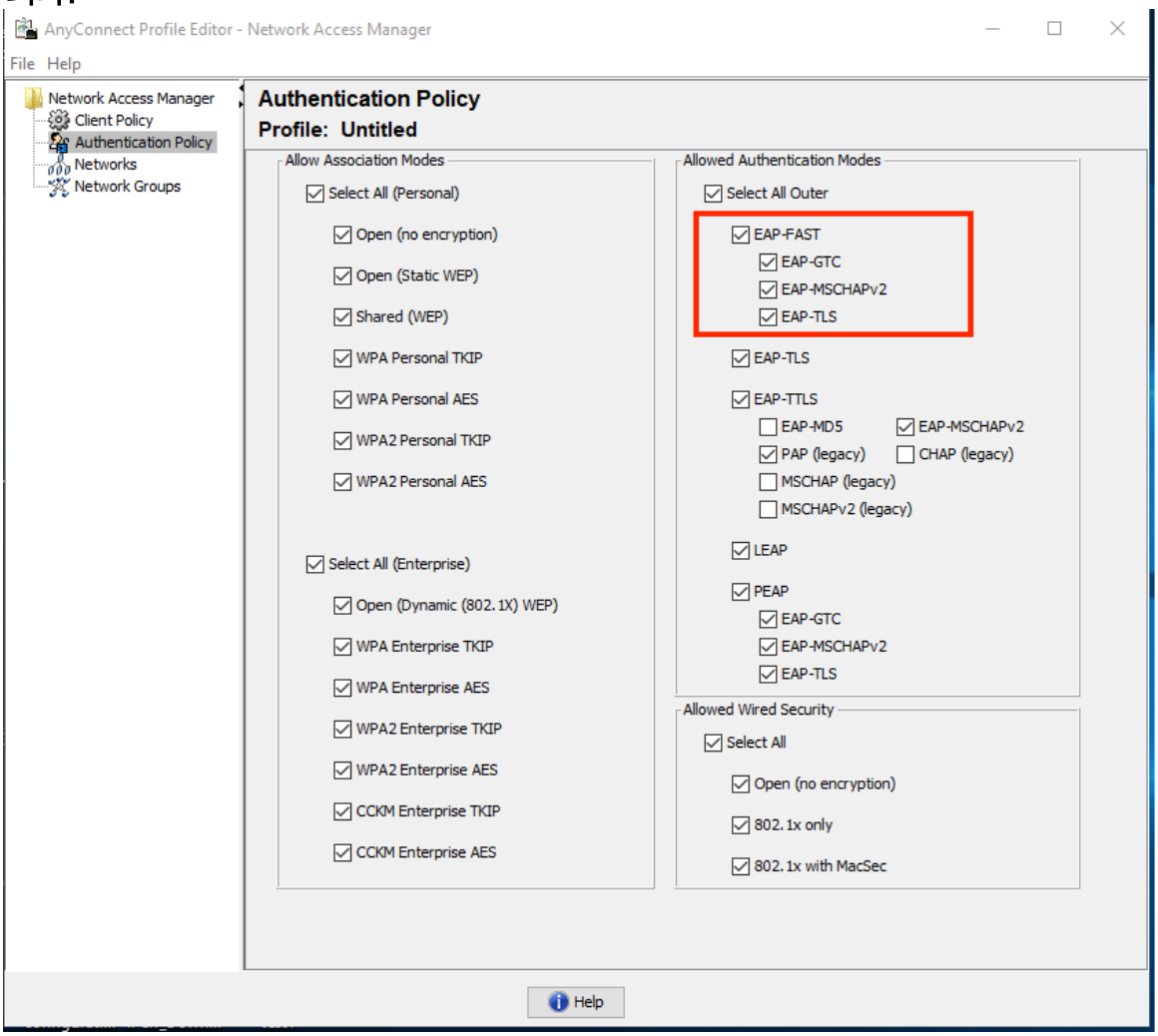
다음을 확인합니다.

이 예에서는 각 WLC 디버그와 함께 Authenticated In-band PAC Provisioning flow 및 NAM(Network Access Manager) 컨피그레이션 설정을 보여줍니다.

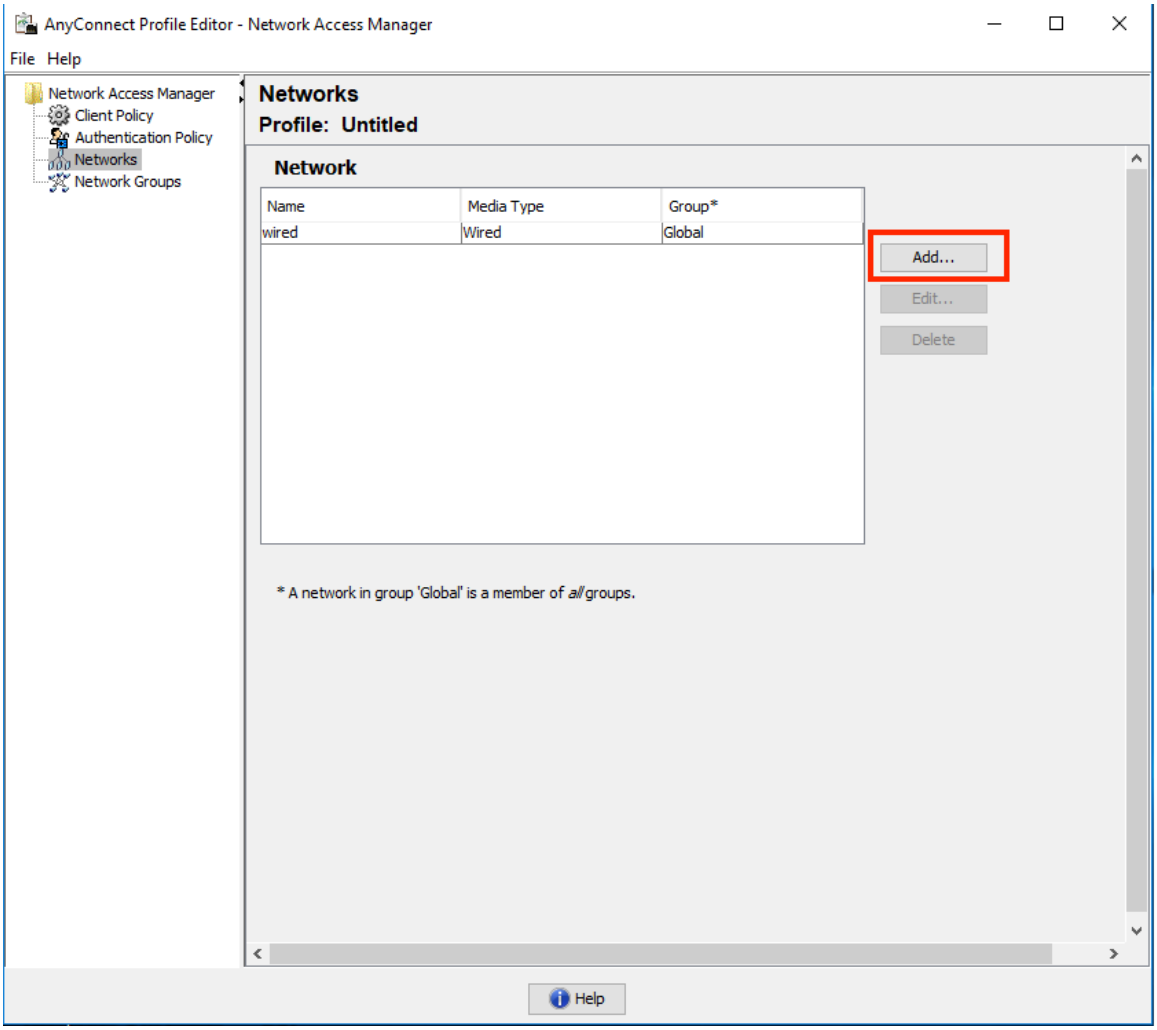
NAM 프로필 컨피그레이션

EAP-FAST를 사용하여 ISE에 대해 사용자 세션을 인증하도록 Anyconnect NAM 프로필을 구성하려면 다음 단계를 수행해야 합니다.

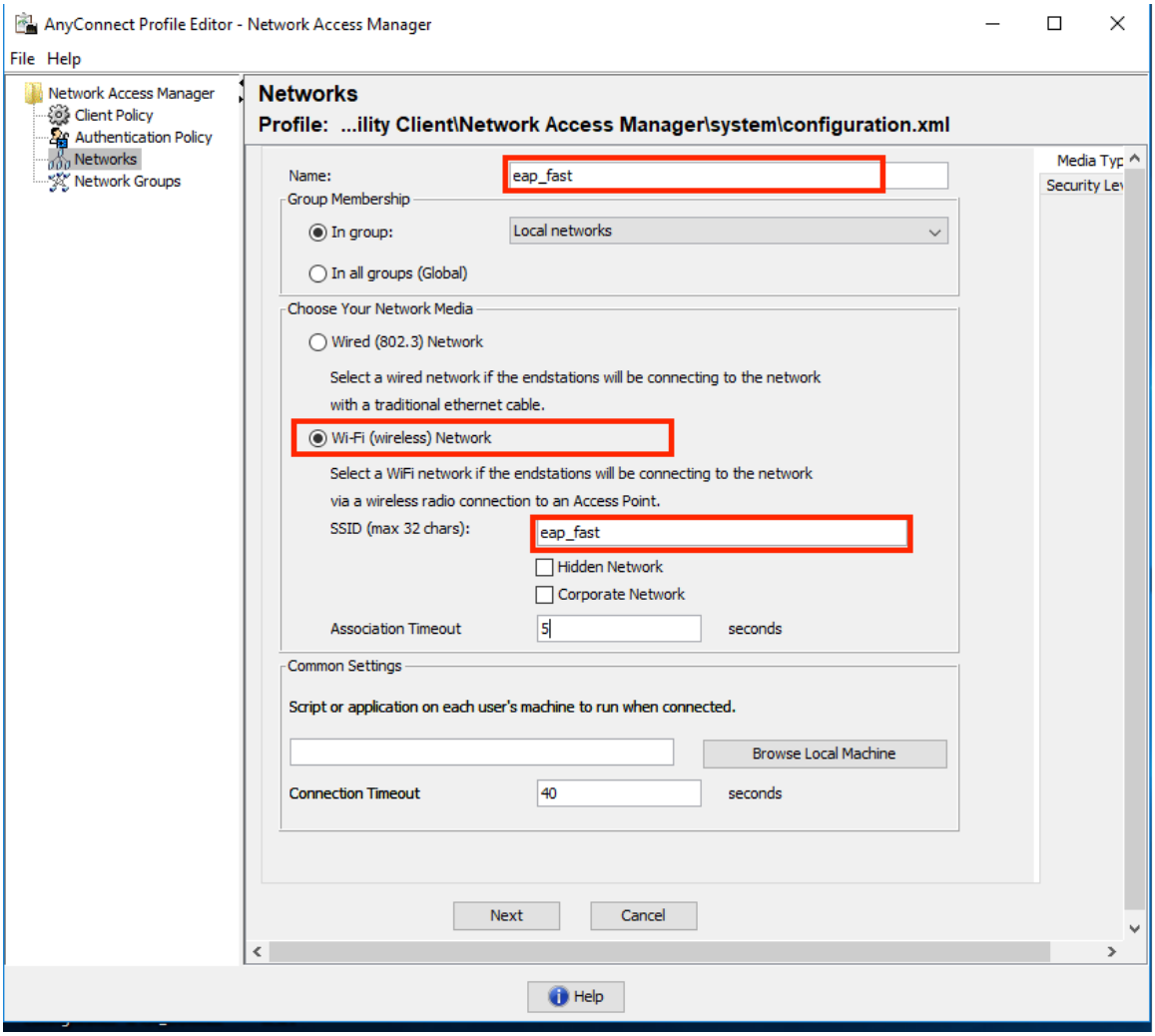
1. Network Access Manager 프로파일 편집기를 열고 현재 구성 파일을 로드합니다.
2. "Allowed Authentication Mode(**인증 모드** 허용)"에서 "**EAP-FAST**"**가 활성화되었는지 확인합니다.**



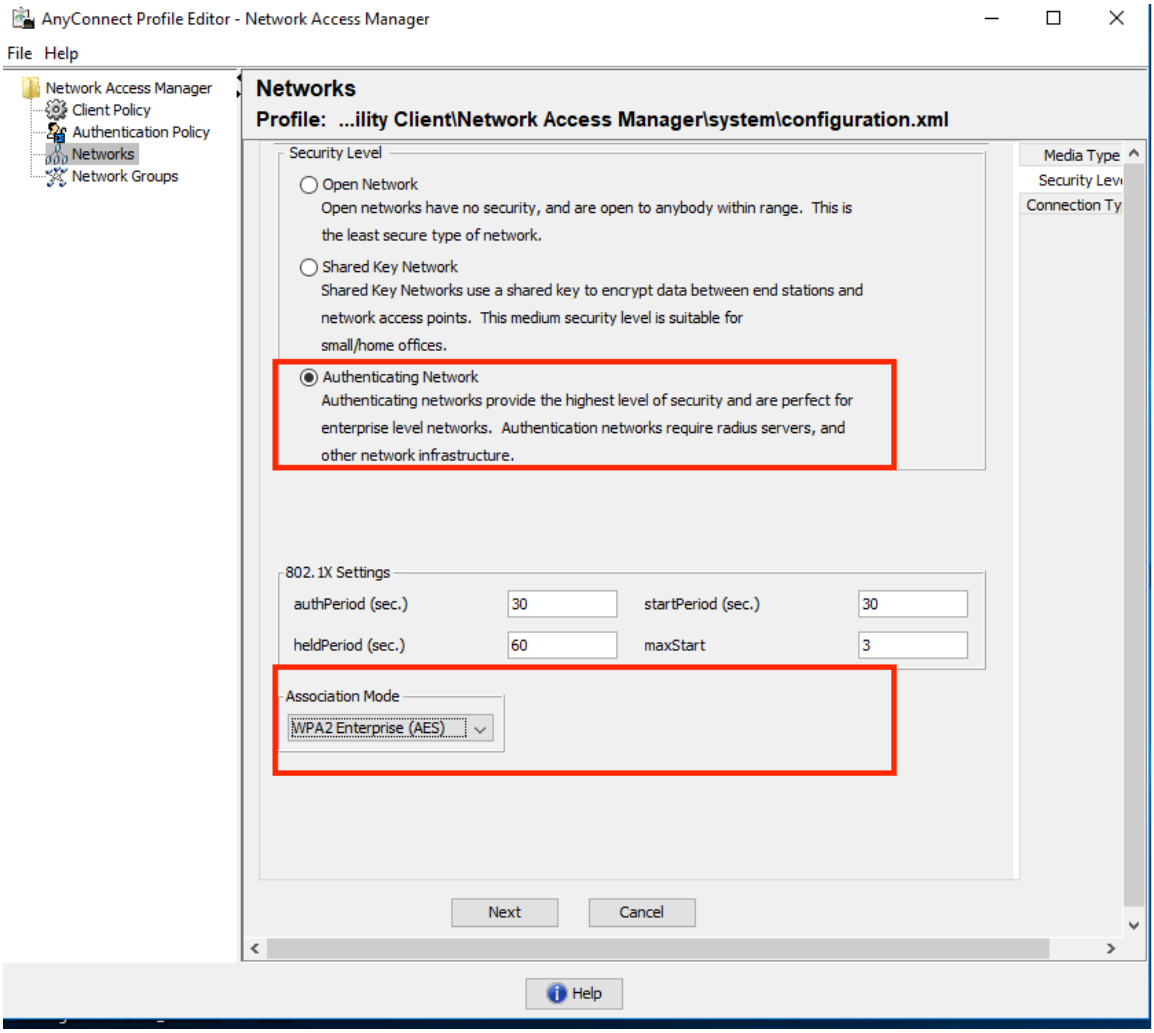
3. "**추가**" 새 네트워크 프로파일:



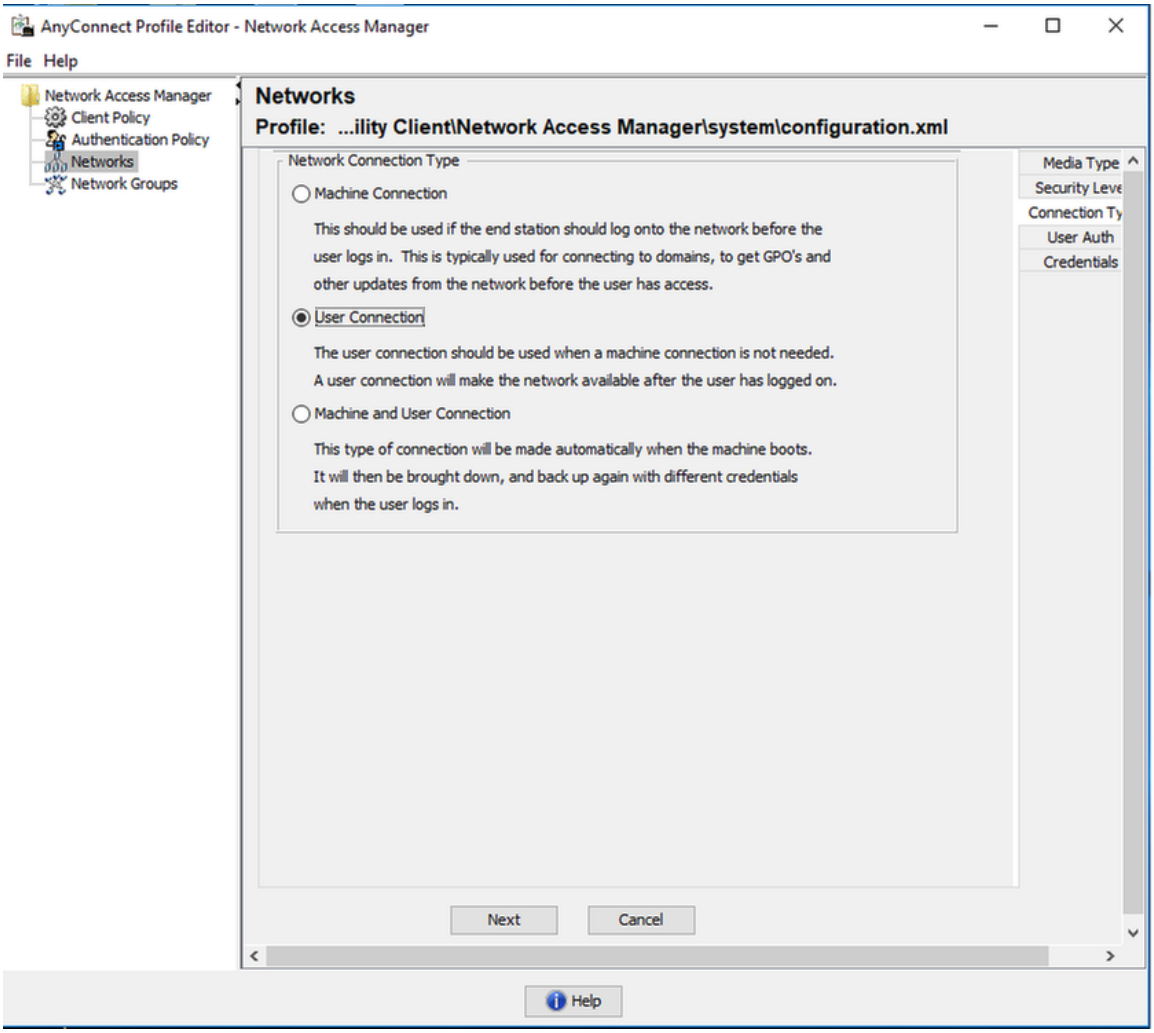
4. "**Media type(미디어 유형)**" 컨피그레이션 섹션에서 "**Name**" 프로파일을 미디어 네트워크 유형으로 정의하고 SSID 이름을 지정합니다.



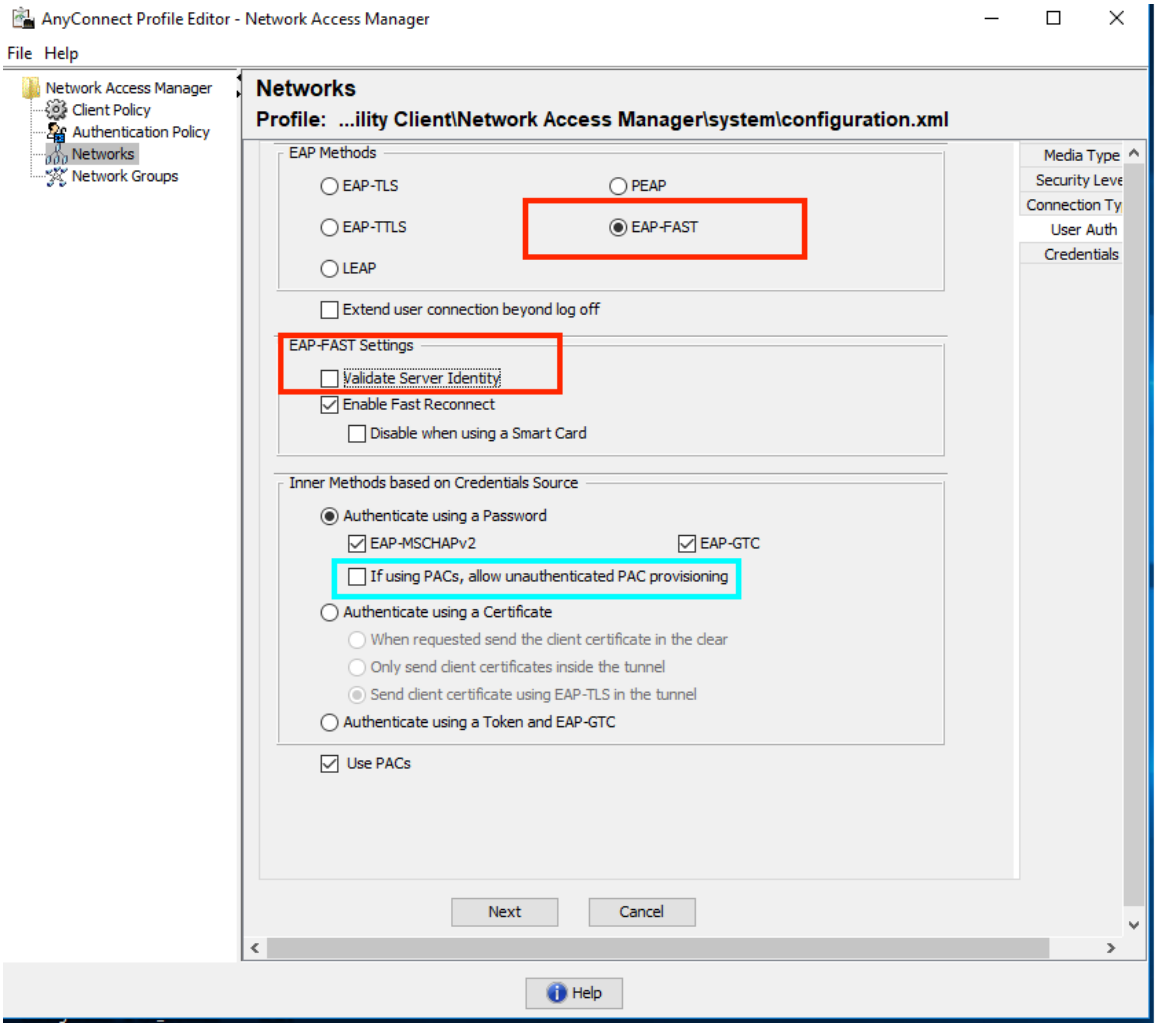
5. "**Security Level(보안 수준)" 구성** 탭에서 "Authenticating Network(인증 네트워크)"를 선택하고 연결 모드를 WPA2 Enterprise(AES)로 지정합니다.



6. 이 예에서는 사용자 유형 인증을 사용합니다. 따라서 다음 탭의 "**연결 유형**"에서 "**사용자 연결 "을** 선택합니다.

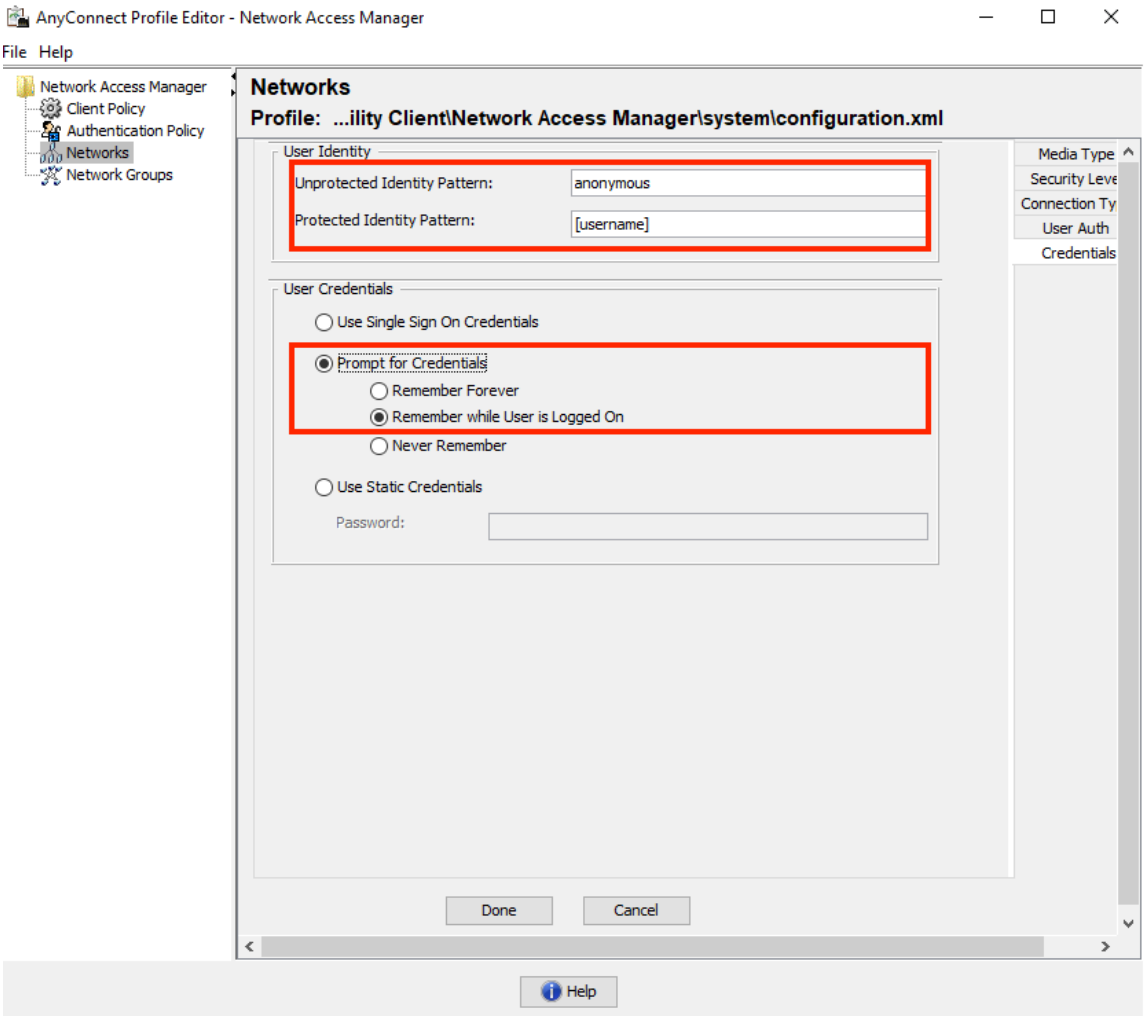


7. "**User Auth**" 탭 아래에서 EAP-FAST를 허용된 인증 방법으로 지정하고 서버 인증서 검증을 비활성화합니다. 이 예에서는 신뢰할 수 있는 인증서를 사용하지 않기 때문입니다.



참고: 실제 프로덕션 환경에서는 ISE에 신뢰할 수 있는 인증서가 설치되어 있는지 확인하고 NAM 설정에서 서버 인증서 검증 옵션을 사용하도록 설정해야 합니다.
참고:"PACs를 사용하는 경우 인증되지 않은 PAC 프로비저닝 허용" 옵션은 익명 대역 내 PAC 프로비저닝의 경우에만 선택해야 합니다.

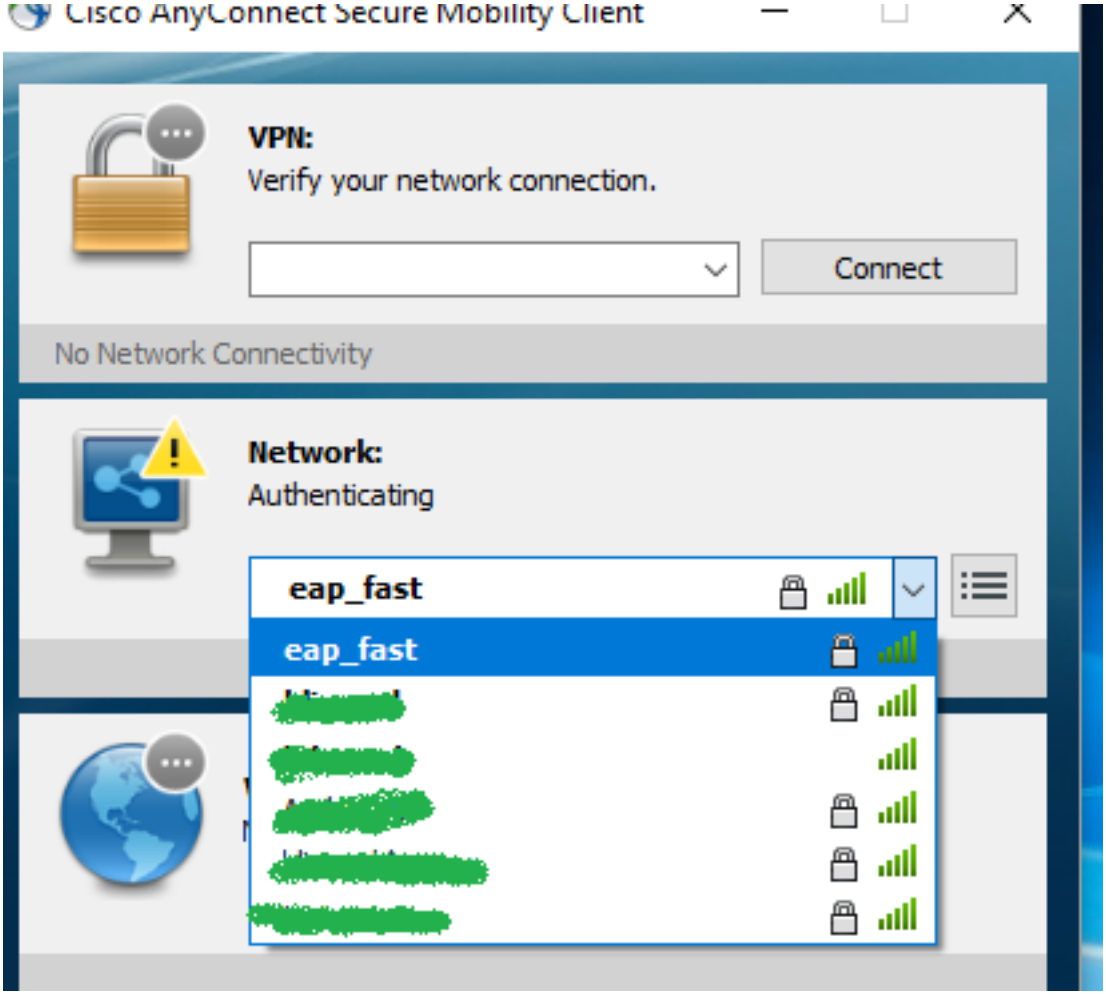
8. 로그인에 사용된 것과 동일한 자격 증명을 사용하려는 경우 사용자 자격 증명을 SSO로 정의하거나, 네트워크에 연결하는 동안 사용자에게 자격 증명을 요청하도록 하거나, 해당 액세스 유형에 대한 정적 자격 증명을 정의하려는 경우 "자격 증명 프롬프트"를 선택합니다.이 예에서는 네트워크에 대한 연결 시도에서 사용자에게 자격 증명을 입력하라는 메시지를 표시합니다.



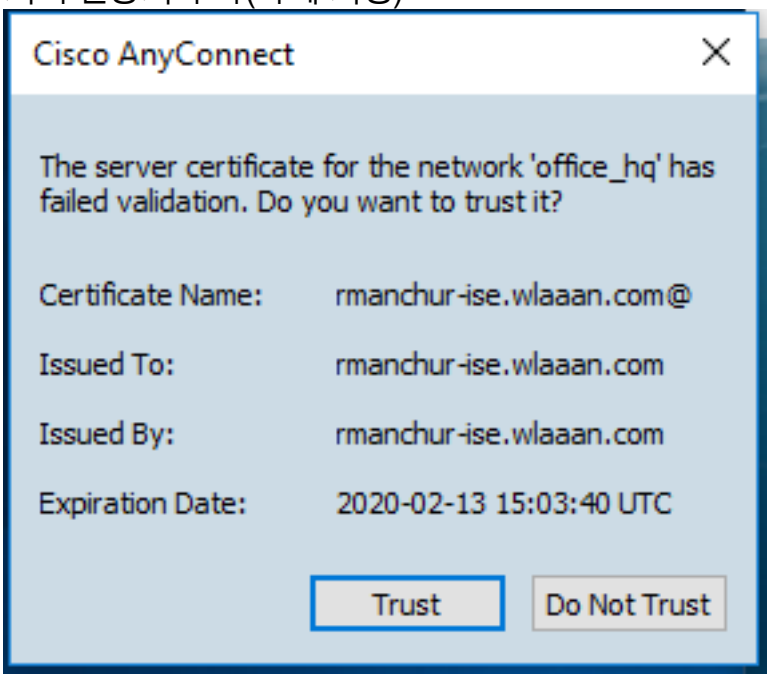
9. 구성된 프로파일을 각 NAM 폴더에 저장합니다.

EAP-FAST 인증을 사용하여 SSID에 대한 연결을 테스트합니다.

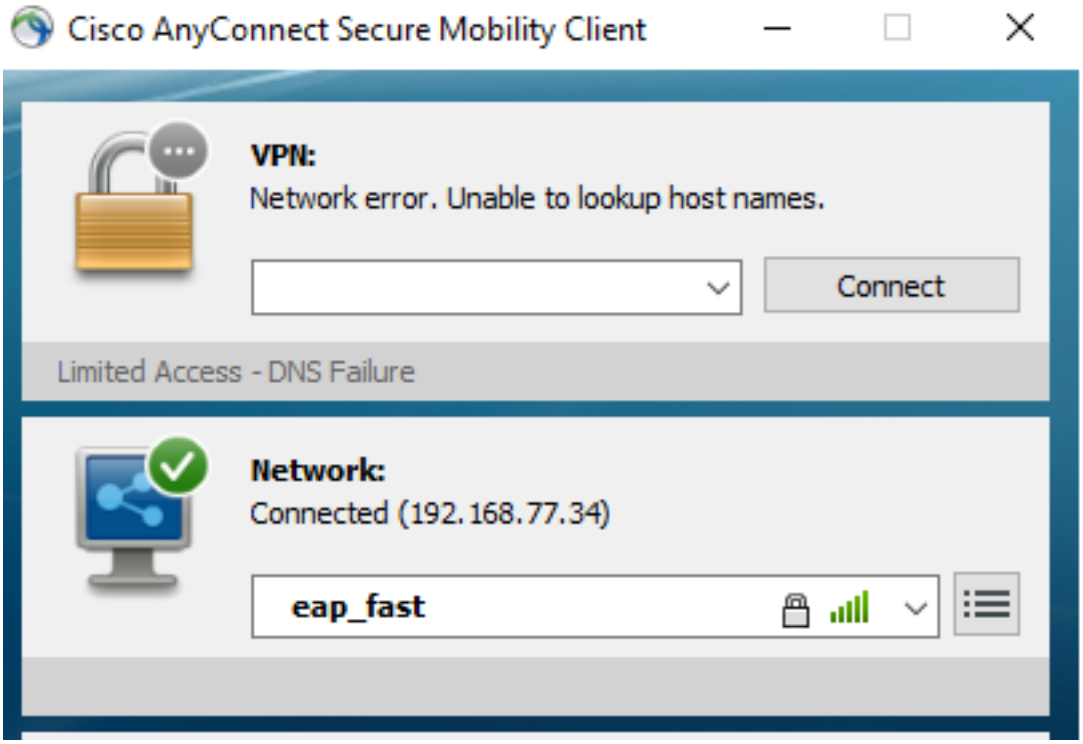
1. AnyConnect 네트워크 목록에서 해당 프로필 선택



2. 인증에 필요한 사용자 이름 및 비밀번호 입력
3. 서버 인증서 수락(자체 서명)



4. 완료



ISE 인증 로그

EAP-FAST 및 PAC 프로비저닝 흐름을 표시하는 ISE 인증 로그는 "**Operations -> RADIUS -> Live Logs**" 아래에서 볼 수 있으며 "**Zoom**" 아이콘을 사용하여 자세한 내용을 볼 수 있습니다.

1. 클라이언트가 인증을 시작했으며 ISE가 EAP-TLS를 인증 방법으로 제안했지만 클라이언트가 거부되고 EAP-FAST를 제안하는 대신 클라이언트와 ISE가 동의한 방법입니다.

Steps

11001	Received RADIUS Access-Request
11017	RADIUS created a new session
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
11507	Extracted EAP-Response/Identity
12500	Prepared EAP-Request proposing EAP-TLS with challenge
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12101	Extracted EAP-Response/NAK requesting to use EAP-FAST instead
12100	Prepared EAP-Request proposing EAP-FAST with challenge
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12102	Extracted EAP-Response containing EAP-FAST challenge-response and accepting EAP-FAST as negotiated

2. PAC 교환을 위해 보호된 환경을 제공하기 위해 클라이언트와 서버 간에 시작된 TLS 핸드셰이크가 성공적으로 완료되었습니다.

12800 Extracted first TLS record; TLS handshake started

12805 Extracted TLS ClientHello message

12806 Prepared TLS ServerHello message

12807 Prepared TLS Certificate message

12808 Prepared TLS ServerKeyExchange message

12810 Prepared TLS ServerDone message

12811 Extracted TLS Certificate message containing client certificate

12105 Prepared EAP-Request with another EAP-FAST challenge

11006 Returned RADIUS Access-Challenge

11001 Received RADIUS Access-Request

11018 RADIUS is re-using an existing session

12104 Extracted EAP-Response containing EAP-FAST challenge-response

12105 Prepared EAP-Request with another EAP-FAST challenge

11006 Returned RADIUS Access-Challenge

11001 Received RADIUS Access-Request (⏰ Step latency=13317 ms)

11018 RADIUS is re-using an existing session

12104 Extracted EAP-Response containing EAP-FAST challenge-response

12812 Extracted TLS ClientKeyExchange message

12813 Extracted TLS CertificateVerify message

12804 Extracted TLS Finished message

12801 Prepared TLS ChangeCipherSpec message

12802 Prepared TLS Finished message

12816 TLS handshake succeeded

3. MS-CHAPv2(사용자 이름/비밀번호 기반 인증)를 사용하여 ISE에서 내부 인증이 시작되었고 사용자 자격 증명이 성공적으로 검증되었습니다.